Michigan Math. J. 66 (2017), 203–219

$(p-1)$th Roots of Unity mod p^n, Generalized Heilbronn Sums, Lind–Lehmer Constants, and Fermat Quotients

Todd Cochrane, Dilum De Silva, & Christopher Pinner

Abstract. For $n \geq 3$, we obtain an improved estimate for the generalized Heilbronn sum $\sum_{x=1}^{p-1} e_{p^n}(yx^{p^{n-1}})$ and use it to show that any interval $\mathcal{I}$ of points in $\mathbb{Z}_{p^n}$ of length $|\mathcal{I}| \gg p^{1.825}$ for $n = 2$, $|\mathcal{I}| \gg p^{2.959}$ for $n = 3$, and $|\mathcal{I}| \geq p^{n-3.269(34/151)^n+o(1)}$ for $n \geq 4$ contains a $(p-1)$th root of unity. As a consequence, we derive an improved estimate for the Lind–Lehmer constant for the Abelian group $\mathbb{Z}_p^n$ and improved estimates for Fermat quotients.

1. Introduction

Let p be a prime, $n \in \mathbb{N}$, $\mathbb{Z}_{p^n}^*$ be the group of units mod p^n, and $G_n \subset \mathbb{Z}_{p^n}^*$ be the subgroup of $(p-1)$th roots of unity,

$$G_n := \{x \in \mathbb{Z}_{p^n}^* : x^{p-1} = 1\} = \{x^{p^{n-1}} \pmod{p^n} : 1 \leq x \leq p-1\}.$$

For $y \in \mathbb{Z}$, let $S_n(y)$ denote the generalized Heilbronn sum

$$S_n(y) := \sum_{x \in G_n} e_{p^n}(yx) = \sum_{x=1}^{p-1} e_{p^n}(yx^{p^{n-1}}),$$

where $e_{p^n}(\cdot) = e^{\frac{2\pi i \cdot}{p^n}}$, and let

$$H_n = \max_{p^n \nmid y} |S_n(y)|.$$

Our interest here is in estimating H_n and studying the distribution of points in G_n. In particular, we wish to determine how large M must be so that any interval

$$\mathcal{I} := \{a+1, \ldots, a+M\} \subset \mathbb{Z}_{p^n} \tag{1.1}$$

of length M is guaranteed to contain an element of G_n. Equivalently, we wish to determine an upper bound on the maximal gap between consecutive $(p-1)$th roots of unity. It is well known that an estimate for H_n leads to a corresponding estimate on the size of the gap. We make this explicit in Corollary 3.1, where we prove that any interval of length $|\mathcal{I}| \geq 3p^{n-1}H_n$ contains an element of G_n.

The current best estimate for H_2 is due to Shkredov [17, Thm. 15],

$$H_2 \ll p^{\frac{5}{6}} \log^{\frac{1}{6}} p, \tag{1.2}$$

Received November 12, 2015. Revision received November 29, 2016.

improving earlier bounds of Heath-Brown [7], Heath-Brown and Konyagin [8], and Shkredov [16], and we make no further improvement here. For $n \geq 3$, Malykhin [14, Cor. 1] obtained $H_n \ll_n p^{1-\frac{3.906}{5^n}}$ for $n \geq 3$. Bourgain and Chang [1, Cor. 4.4] also obtained a nontrivial bound of the type $H_n \ll p^{1-\delta_n}$ for some undetermined constant $\delta_n > 0$, as a special case of their very general exponential sum estimate over subgroups of $\mathbb{Z}_m^*$ with m composite. Here, we use the bound for H_2 in (1.2) and a recent energy estimate of Shkredov, Solodkova, and Vyugin [18] to refine the estimate of Malykhin, obtaining in Theorem 8.1 and Corollary 8.1

$$H_3 \ll p^{1-\frac{29}{702}+o(1)} = p^{0.95868\ldots+o(1)}; \tag{1.3}$$

$$H_n \ll p^{1-3.269(\frac{34}{151})^n+o(1)} \quad \text{for } n \geq 4. \tag{1.4}$$

The same estimate for H_3 was also obtained recently by Shteinikov [21, Thm. 13] in a similar manner.

From Corollary 3.1 we immediately deduce the following result for $n \geq 3$.

THEOREM 1.1. *Any interval $\mathcal{I} \subset \mathbb{Z}_{p^n}$ of length as further given in* (1.5) *contains an element of G_n*

$$|\mathcal{I}| \geq \begin{cases} p^{2-\frac{575}{3276}+o(1)} & \text{if } n = 2; \\ p^{3-\frac{29}{702}+o(1)} & \text{if } n = 3; \\ p^{n-3.269(\frac{34}{151})^n+o(1)} & \text{if } n \geq 4. \end{cases} \tag{1.5}$$

To be precise, for $n = 2$, the $o(1)$ is an undetermined function of p that goes to 0 as $p \to \infty$, whereas for $n \geq 3$, $o(1) = c_n \log\log p/\log p$ for some effectively computable constant c_n. The estimate given for the case $n = 2$ does not follow from Theorem 3.1, but requires instead a method of Konyagin and Shparlinski [10] given in Section 4; the proof for $n = 2$ is given in Section 5. As a consequence of the theorem, we obtain an improved estimate for the Lind–Lehmer constant for the Abelian group $\mathbb{Z}_p^n$ (Sect. 2) and improved estimates for Fermat quotients (Sect. 6).

2. The Lind–Lehmer Constant for Finite Abelian Groups

Our interest in the distribution of elements of G_n was originally motivated by the problem of determining the Lind–Lehmer constant for the group $\mathbb{Z}_p^n$.

For a polynomial $F(x) = a_0 \prod_{i=1}^n (x - \alpha_i) \in \mathbb{C}[x]$, we define the traditional Mahler measure $M(F) = |a_0| \prod_{i=1}^n \max\{1, |\alpha_i|\}$ and the logarithmic Mahler measure $m(F) = \log M(F)$. Famously, Lehmer [11] asked whether there exists a constant $c > 0$ such that, for any polynomial F in $\mathbb{Z}[x]$, either $m(F) = 0$ or $m(F) > c$. By Jensen's formula we can write

$$m(F) = \int_0^1 \log|F(e^{2\pi i x})|\, dx,$$

allowing us to generalize the concept of Mahler measure to $F \in \mathbb{C}[x_1, \ldots, x_n]$:

$$m(F) := \int_0^1 \cdots \int_0^1 \log |F(e^{2\pi i x_1}, \ldots, e^{2\pi i x_n})| \, dx_1 \cdots dx_n. \tag{2.1}$$

Since (see, e.g., Boyd [4])

$$m(F(x_1, x_2, \ldots, x_n)) = \lim_{k \to +\infty} m(F(x, x^k, x^{k^2}, \ldots, x^{k^{n-1}})),$$

the infimum of positive measures over polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$ reduces to the classical one-variable Lehmer problem.

Lind [13], viewing (2.1) as an integral over the group $\mathbb{R}/\mathbb{Z} \times \cdots \times \mathbb{R}/\mathbb{Z}$ and $F(e^{2\pi i x_1}, \ldots, e^{2\pi i x_n})$ as a linear sum of characters on that group, generalized the concept of Mahler measure to an arbitrary compact Abelian group G with normalized Haar measure μ and dual group of characters $\hat{G}$, defining, for an f in $\mathbb{Z}[\hat{G}]$,

$$m_G(f) = \int_G \log |f| \, d\mu.$$

Analogously to the Lehmer problem, we can ask what is the smallest positive measure for that group and define the Lind–Lehmer constant

$$\lambda(G) := \inf\{m_G(f) : f \in \mathbb{Z}[\hat{G}], m_G(f) > 0\}.$$

For example, for a finite Abelian group

$$G = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$$

and $F \in \mathbb{C}[x_1, \ldots, x_n]$, we can define, as a natural counterpart to (2.1), the measure

$$m_G(F) = \frac{1}{|G|} \sum_{j_1=1}^{m_1} \cdots \sum_{j_n=1}^{m_n} \log |F(e^{2\pi i j_1/m_1}, \ldots, e^{2\pi i j_n/m_n})|,$$

and $\lambda(G)$ will be the minimum positive measure $m_G(F)$ over the $F \in \mathbb{Z}[x_1, \ldots, x_n]$.

In [5] the latter two authors showed that

$$\lambda(\mathbb{Z}_2^n) = \frac{1}{2^n} \log(2^n - 1)$$

and, for an odd prime p, that

$$\lambda(\mathbb{Z}_p^n) = \frac{1}{p^n} \log \mathcal{M}_n,$$

where

$$\mathcal{M}_n := \min\{2 \le a \le p^n - 1 : a \in G_n\}.$$

Thus, an upper bound on the Lehmer constant $\lambda(\mathbb{Z}_p^n)$ will follow at once from any limitation on the size of an interval not containing an element of G_n. In the next section we relate this to bounds on the Heilbronn sums; in particular, we show that

$$\mathcal{M}_n \le 3p^{n-1} H_n.$$

3. Using Estimates for H_n to Estimate Gap Sizes

In this section we use the standard method to obtain a basic theorem relating the distribution of elements of G_n to the estimation of the Heilbronn sum. In fact, the result we obtain can be stated for any subgroup G of $\mathbb{Z}_{p^n}^*$. Set

$$\Phi_G = \max_{p^n \nmid y} \left| \sum_{x \in G} e_{p^n}(yx) \right|.$$

THEOREM 3.1. *For any prime power p^n and subgroup G of $\mathbb{Z}_{p^n}^*$, any interval $\mathcal{I} \subset \mathbb{Z}_{p^n}$ of length $|\mathcal{I}| \geq 2(\Phi_G/|G|)p^n$ contains an element of G.*

Applying the theorem to G_n and using the fact that $|G_n| = p - 1 \geq \frac{2}{3}p$ for odd p, we obtain the following corollary. (The statement is trivial for $p = 2$.)

COROLLARY 3.1. *For any prime power p^n, any interval $\mathcal{I} \subset \mathbb{Z}_{p^n}$ of length $|\mathcal{I}| \geq 3p^{n-1}H_n$ contains an element of G_n.*

Proof of Theorem 3.1. Let $\alpha : \mathbb{Z}_{p^n} \to \mathbb{R}$ be a real-valued function supported on an interval $\mathcal{I}$ as given in (1.1). If we can show that $\sum_{x \in G} \alpha(x) > 0$, then it follows that $G \cap \mathcal{I}$ is nonempty. To this end, we let $\alpha(x) = \sum_{y=1}^{p^n} a(y) e_{p^n}(yx)$ be the Fourier expansion of α, where for any y, $a(y) = p^{-n} \sum_{x=1}^{p^n} e_{p^n}(-yx)\alpha(x)$. Also, for any integer y, put

$$S(y) := \sum_{x \in G} e_{p^n}(yx).$$

Then

$$\begin{aligned} \sum_{x \in G} \alpha(x) &= \sum_{x \in G} \sum_{y=1}^{p^n} a(y) e_{p^n}(yx) \\ &= p^{-n}|G| \sum_{x=1}^{p^n} \alpha(x) + \sum_{y=1}^{p^n - 1} a(y)S(y) := M_\alpha + E_\alpha, \end{aligned} \tag{3.1}$$

say. We call M_α the main term of (3.1), and E_α the error term.

The simplest way to bound the error term E_α is just to say

$$|E_\alpha| \leq \sum_{y=1}^{p^n - 1} |a(y)S(y)| \leq \Phi_G \sum_{y=1}^{p^n - 1} |a(y)|. \tag{3.2}$$

We apply this estimate to the weighted function $\alpha = 1_{\mathcal{J}} * 1_{\mathcal{K}}$, where

$$\mathcal{J} = \{1, 2, \ldots, \lceil M/2 \rceil\}, \qquad \mathcal{K} = \{a, \ldots, a + \lfloor M/2 \rfloor\}.$$

Here, $1_{\mathcal{J}}$ and $1_{\mathcal{K}}$ are the characteristic functions of the intervals $\mathcal{J}$ and $\mathcal{K}$, say with Fourier coefficients $a_{\mathcal{J}}(y)$ and $a_{\mathcal{K}}(y)$ respectively, and $*$ denotes convolution. We note that α is supported on $\mathcal{I}$,

$$M_\alpha = p^{-n}|G|\sum_{x=1}^{p^n}\alpha(x) = p^{-n}|G||\mathcal{J}||\mathcal{K}|,$$

and that

$$a(y) = p^n a_{\mathcal{J}}(y)a_{\mathcal{K}}(y).$$

Thus, by the Cauchy–Schwarz inequality and Parseval identity,

$$\sum_{y=1}^{p^n}|a(y)| = p^n\sum_{y=1}^{p^n}|a_{\mathcal{J}}(y)||a_{\mathcal{K}}(y)| \le p^n\left(\sum_{y=1}^{p^n}|a_{\mathcal{J}}(y)|^2\right)^{1/2}\left(\sum_{y=1}^{p^n}|a_{\mathcal{K}}(y)|^2\right)^{1/2}$$

$$= p^n p^{-n}\left(\sum_{x=1}^{p^n}|1_{\mathcal{J}}(x)|^2\right)^{1/2}\left(\sum_{x=1}^{p^n}|1_{\mathcal{K}}(x)|^2\right)^{1/2} = |\mathcal{J}|^{1/2}|\mathcal{K}|^{1/2},$$

and so the main term M_α in (3.1) exceeds the error term E_α, provided that

$$p^{-n}|G||\mathcal{J}||\mathcal{K}| > \Phi_G|\mathcal{J}|^{1/2}|\mathcal{K}|^{1/2},$$

that is,

$$|\mathcal{J}||\mathcal{K}| > (\Phi_G/|G|)^2 p^{2n}.$$

Since $|\mathcal{J}||\mathcal{K}| = \lceil M/2\rceil(1+\lfloor M/2\rfloor) > M^2/4$, we see that it suffices to have $M \ge 2(\Phi_G/|G|)p^n$, establishing the theorem. □

4. Improving the Error Estimate

We can improve the estimate of the error term in certain cases using a method of Konyagin and Shparlinski [10, Chap. 7]. The same method was also used for related problems in [3] and [2]. Let $q = p^n$, and G be any subgroup of $\mathbb{Z}_q^*$. Partition $\mathbb{Z}_q^*$ into the different cosets of G:

$$\mathbb{Z}_q^* = Gy_1 \cup Gy_2 \cup \cdots \cup Gy_L,$$

where $L = (p^n - p^{n-1})/|G|$. Fix a parameter $h < p$, to be determined later, and let

$$N_i := \#\{y \in Gy_i : 0 < |y| \le h\}$$

and

$$\phi_i := |S(y_i)|.$$

It is plain that ϕ_i just depends on the coset Gy_i and not on the representative y_i. Let

$$\alpha = 1_{\mathcal{J}_1} * 1_{\mathcal{J}_2} * \cdots * 1_{\mathcal{J}_k},$$

where the $\mathcal{J}_i$ are intervals of length $m = \lfloor \frac{M}{k} \rfloor$, chosen so that α is supported on $\mathcal{I}$. Then the Fourier coefficients of α satisfy

$$a(0) = q^{-1}m^k,$$

and for any $y \neq 0$ with $|y| \leq q/2$, we have

$$|a(y)| = \frac{1}{q}\frac{|\sin^k(\pi ym/q)|}{|\sin^k(\pi y/q)|} \leq \min\left\{\frac{m^k}{q}, \frac{q^{k-1}}{2^k|y|^k}\right\}. \tag{4.1}$$

Thus, to estimate the error term in (3.1), we write

$$\begin{aligned}|E_\alpha| &= \left|\sum_{y=1}^{q-1} a(y)S(y)\right| = \left|\sum_{0<|y|\leq q/2} a(y)S(y)\right| \\ &\leq \sum_{0<|y|\leq h} |a(y)||S(y)| + \sum_{h<|y|\leq q/2} |a(y)||S(y)| = \Sigma_1 + \Sigma_2,\end{aligned}$$

say. Noting that, for $0 < |y| \leq h < p$, we must have $y \in \mathbb{Z}_q^*$, we obtain

$$\Sigma_1 \leq \frac{m^k}{q}\sum_{0<|y|<h}|S(y)| = \frac{m^k}{q}\sum_{i=1}^{L}\sum_{\substack{0<|y|<h\\ y\in Gy_i}}\phi_i = \frac{m^k}{q}\sum_{i=1}^{L}N_i\phi_i, \tag{4.2}$$

whereas for Σ_2, by the definition of Φ_G and (4.1) we have

$$\begin{aligned}\Sigma_2 &\leq \max_{y\neq 0}|S(y)| \sum_{h\leq|y|\leq q/2}\frac{q^{k-1}}{2^k|y|^k} \leq \Phi_G\frac{q^{k-1}}{2^{k-1}}\left(\frac{1}{h^k} + \frac{1}{(k-1)h^{k-1}}\right) \\ &\leq \frac{\Phi_G q^{k-1}(k+h-1)}{2^{k-1}h^k(k-1)}.\end{aligned}$$

We succeed with this method provided that $\Sigma_1 \leq \frac{1}{2}M_\alpha$ and $\Sigma_2 < \frac{1}{2}M_\alpha$, with M_α the main term in (3.1),

$$M_\alpha = q^{-1}|G|\sum_x \alpha(x) = q^{-1}|G|m^k.$$

Thus, it suffices to have

$$\frac{\Phi_G q^{k-1}(k+h-1)}{2^{k-1}h^k(k-1)} < \frac{m^k|G|}{2q} \quad \text{and} \quad \frac{m^k}{q}\sum_{i=1}^{L}N_i\phi_i \leq \frac{|G|m^k}{2q}$$

or, equivalently,

$$m > \left(\frac{4\Phi_G(k+h-1)}{|G|(k-1)}\right)^{\frac{1}{k}}\frac{q}{2h} \quad \text{and} \quad \sum_{i=1}^{L}N_i\phi_i \leq \frac{|G|}{2}.$$

Taking $k = \lceil \log p \rceil$ and observing that

$$\left(\frac{4\Phi_G(k+h-1)}{|G|(k-1)}\right)^{\frac{1}{k}} \leq \left(\frac{4(k+h-1)}{k-1}\right)^{\frac{1}{k}} \leq \left[4\left(1+\frac{p}{\lfloor \log p\rfloor}\right)\right]^{\frac{1}{\lceil \log p\rceil}} < 6$$

(the maximum value of the latter expression, 5.2915..., occurring at $p = 7$), we see that the first condition holds provided that $m \geq \frac{3q}{h}$. Thus, we arrive at the following generalization and refinement of [10, Lemma 7.1], which was stated for the case of subgroups of $\mathbb{Z}_p^*$.

PROPOSITION 4.1. *Suppose that* $q = p^n$ *is a prime power,* G *is a subgroup of* $\mathbb{Z}_q^*$, *and that* $h < p$ *is such that* $\sum_{i=1}^{L} N_i\phi_i < \frac{|G|}{2}$. *Then any interval of length* $M \geq \lceil \frac{3q}{h} \rceil \lceil \log p \rceil$ *contains a point in* G.

In comparison, the result of [10, Lemma 7.1] for $n = 1$ requires $M \gg_\varepsilon p^{1+\varepsilon}/h$ for the same conclusion.

We can estimate the sum $\sum_{i=1}^{L} N_i\phi_i$ using the Hölder inequality:

$$\sum_{i=1}^{L} N_i\phi_i \leq \Big(\sum_{i=1}^{L} N_i\Big)^{\frac{1}{2}} \Big(\sum_i N_i^2\Big)^{\frac{1}{4}} \Big(\sum_{i=1}^{L} \phi_i^4\Big)^{\frac{1}{4}}. \tag{4.3}$$

Now

$$\sum_{i=1}^{L} N_i = \sum_{i=1}^{L} \sum_{\substack{y \in Gy_i \\ |y| \leq h}} 1 = \sum_{\substack{y \in \mathbb{Z}_q^* \\ |y| \leq h}} 1 \leq 2h,$$

$$\sum_{i=1}^{L} N_i^2 = \sum_{i=1}^{L} \#\{(y,z) : y, z \in Gy_i, |y| \leq h, |z| \leq h\} = N(h),$$

where

$$N(h) := \#\{(y,z) : y/z \in G, |y| \leq h, |z| \leq h\},$$

and

$$\sum_{i=1}^{L} \phi_i^4 = \sum_{i=1}^{L} \Big|\sum_{x \in G} e_q(y_i x)\Big|^4 = \frac{1}{|G|} \sum_{y \in \mathbb{Z}_q^*} \Big|\sum_{x \in G} e_q(yx)\Big|^4$$

$$\leq \frac{1}{|G|} \sum_{y \in \mathbb{Z}_q} \Big|\sum_{x \in G} e_q(yx)\Big|^4 = \frac{q}{|G|} T_2(G),$$

where $T_2(G)$ is the additive energy of G,

$$T_2(G) := \#\{(x_1, x_2, y_1, y_2) : x_i, y_i \in G, x_1 + x_2 = y_1 + y_2\}.$$

Thus, by (4.3) we have

$$\sum_{i=1}^{L} N_i\phi_i \leq (2h)^{\frac{1}{2}} N(h)^{\frac{1}{4}} (q/|G|)^{\frac{1}{4}} T_2(G)^{\frac{1}{4}}. \tag{4.4}$$

In order to proceed further, we need good estimates for $N(h)$ and for $T_2(G)$. Bourgain, Konyagin, and Shparlinski [3, Thm. 1] established that, for any non-negative integer q, subgroup G of $\mathbb{Z}_q^*$, and positive integer ν,

$$N(h) \leq hq^{\frac{1}{4\nu(\nu+1)}+o(1)} + h^2 q^{-\frac{1}{2\nu}+o(1)},$$

where the $o(1)$ indicates a function that tends to zero as $q \to \infty$. The optimal choice for our application is $\nu = 6$, where we have

$$N(h) \leq hq^{\frac{1}{168}+o(1)} + h^2 q^{-\frac{1}{12}+o(1)}. \tag{4.5}$$

In the next section we apply this estimate to the subgroup G_2 of $(p-1)$th roots of unity in $\mathbb{Z}^*_{p^2}$.

5. Proof of the Case $n = 2$ of Theorem 1.1

Inserting the bound for $N(h)$ into (4.5) and the current record breaking bound for $T_2(G_2)$ of Shkredov, Solodkova, and Vyugin [18, Thm. 24],

$$T_2(G_2) \ll p^{\frac{32}{13}} \log^{\frac{14}{13}} p \ll p^{2.46153\ldots+o(1)}, \tag{5.1}$$

from (4.4) we obtain

$$\begin{aligned}\sum_{i=1}^{L} N_i \phi_i &\ll h^{\frac12}(h^{\frac14} p^{\frac{1}{336}+o(1)} + h^{\frac12} p^{-\frac{1}{24}+o(1)}) p^{\frac14} (p^{\frac{32}{13}} \log^{\frac{14}{13}} p)^{\frac14} \\ &\le h^{\frac34} p^{\frac{3793}{4368}+o(1)} + h p^{\frac{257}{312}+o(1)}. \end{aligned}\tag{5.2}$$

Thus, Proposition 4.1 applies, provided that $h \ll p^{\frac{575}{3276}+o(1)}$, and so we see that any interval of length $|\mathcal{I}| \ge p^{\frac{5977}{3276}+o(1)} = p^{1.82448\ldots+o(1)}$ contains a pth power, proving the case $n = 2$ of Theorem 1.1.

REMARK 5.1. It is conjectured [3] that, for $\varepsilon > 0$ and $h < p^{n-1}$,

$$N(h) \ll_\varepsilon h q^\varepsilon. \tag{5.3}$$

See also an analogous conjecture in [10, Quest. 7.8] for the case of prime moduli. Such a bound follows from GRH as we demonstrate in the following proposition. If we use the conjectured upper bound on $N(h)$ in the previous argument, then we would obtain the improvement $|\mathcal{I}| \ge p^{\frac{49}{27}+\varepsilon} = p^{1.81481\ldots+\varepsilon}$.

PROPOSITION 5.1. *On the assumption of GRH, we have that, for $h < q$,*

$$N(h) \ll_\varepsilon \frac{h^2}{p^{n-1}} + h q^\varepsilon.$$

Proof. We have

$$\begin{aligned} N(h) &= \frac{1}{p^{n-1}} \sum_{|y|\le h} \sum_{|z|\le h} \sum_{\chi^{p^{n-1}}=\chi_0} \chi(y/z) \\ &\ll \frac{h^2}{p^{n-1}} + \frac{1}{p^{n-1}} \sum_{\substack{\chi^{p^{n-1}}=\chi_0 \\ \chi\ne\chi_0}} \left|\sum_{y=1}^{h} \chi(y)\right|^2 \\ &\ll_\varepsilon \frac{h^2}{p^{n-1}} + \frac{1}{p^{n-1}} p^{n-1}(h^{1/2} q^\varepsilon)^2, \end{aligned}$$

the latter inequality being a consequence of GRH, as noted by Montgomery and Vaughan [15]. □

REMARK 5.2. The estimate for $n = 2$ has strong parallels with the following result of Shteinikov [21, Thm. 10] for subgroups of $\mathbb{Z}_p^*$. We restate his result in the notation of this paper.

THEOREM 5.1. *Let G be a subgroup of $\mathbb{Z}_p^*$ of order $|G| \geq \sqrt{p}$. Then any interval $\mathcal{I}$ of length $|\mathcal{I}| \geq p^{\frac{5977}{6552}+o(1)}$ contains an element of G.*

The square root threshold needed for applying the theorem, in the context of subgroups of $\mathbb{Z}_{p^n}^*$, is satisfied by G_2 when $n = 2$, where $|G_2| = (p-1)$ is roughly $\sqrt{p^2}$, but fails for G_n with $n > 2$. This is why we were able to obtain the improvement for $n = 2$ but not for $n > 2$. The proof in [21] follows a similar line of argument as our proof before for $n = 2$. Indeed, its main appeal is to the result of Konyagin and Shparlinski [10, Lemma 7.1] (analogous to our Prop. 4.1) and to the estimate of Bourgain, Konyagin, and Shparlinski in (4.5) (with $q = p$).

6. Fermat Quotients

For prime power p^n with $n \geq 2$ and integer u with $p \nmid u$, we define the Fermat quotient $q_{p^{n-1}}(u)$ to be the unique integer with $0 \leq q_{p^{n-1}}(u) \leq p^{n-1} - 1$ and

$$q_{p^{n-1}}(u) \equiv \frac{u^{p-1} - 1}{p} \pmod{p^{n-1}}.$$

It is plain that $q_{p^{n-1}}$ is constant on any coset of G_n and that it takes on distinct values on distinct cosets of G_n. Thus, the Fermat quotients take on all values from 0 to $p^{n-1} - 1$ as u runs through a complete residue system mod p^n. Following Shparlinski [19], we define $\Lambda_{p^{n-1}}$ to be the minimal value L such that, on any interval of length L, $q_{p^{n-1}}(u)$ takes on a full spectrum of values from 0 to $p^{n-1} - 1$,

$$\Lambda_{p^{n-1}} := \min\{L : \forall K \in \mathbb{Z}, \text{ we have } \#\{q_{p^{n-1}}(K+1), \ldots, q_{p^{n-1}}(K+L)\} = p^{n-1}\}.$$

A value L is permissable if for any coset of G_n and any interval $\mathcal{I}$ of length L, $\mathcal{I}$ contains an element of the coset. It is plain from the proof of Theorem 1.1 that the theorem holds identically with G_n replaced with any coset of G_n. Thus we obtain the following:

THEOREM 6.1. *We have*

$$\Lambda_{p^{n-1}} \leq \begin{cases} p^{2-\frac{575}{3276}+o(1)} & \text{if } n = 2; \\ p^{3-\frac{29}{702}+o(1)} & \text{if } n = 3; \\ p^{n-3.269(\frac{34}{151})^n+o(1)} & \text{if } n \geq 4. \end{cases}$$

The theorem improves on a result of Shparlinski, who obtained, for $n = 2$, the estimate $\Lambda_p \leq p^{\frac{463}{252}+o(1)}$.

Of perhaps greater interest in the study of Fermat quotients is the determination of ℓ_p, the minimal positive value of u for which $q_p(u) \neq 0$. Lenstra [12] obtained the uniform upper bound $\ell_p \leq 4\log^2 p$ for all primes p. This was improved by Bourgain, Ford, Konyagin, and Shparlinski [2] to $\ell_p \leq (\log p)^{\frac{463}{252}+o(1)}$ as $p \to \infty$, by Shkredov [16] to $\ell_p \leq (\log p)^{\frac{7829}{4284}+o(1)}$, and by Shkredov, Solodkova, and Vyugin [18, Thm. 28] to $\ell_p \leq (\log p)^{\frac{5977}{3276}+o(1)} = (\log p)^{1.82448\ldots+o(1)}$. Sharper estimates have been obtained that hold for almost all primes, $\ell_p \leq (\log p)^{\frac{5}{3}+\varepsilon}$ in [2] and $\ell_p \leq (\log p)^{\frac{3}{2}+\varepsilon}$ in [20]. Granville [6, Conj. 10] conjectured that $\ell_p = o(\log^{\frac{1}{4}} p)$. Lenstra [12] suggested that the truth may in fact be $\ell_p \leq 3$ for all p.

Here, we generalize the problem to any prime power p^n with $n \geq 2$, defining $\ell_{p^{n-1}}$ to be the minimal positive integer u such that p^n is not a divisor of $u^{p-1}-1$, that is, $u \notin G_n$.

THEOREM 6.2. (i) *We have* $\ell_p \leq (\log p)^{2-\frac{575}{3276}+o(1)}$ *as* $p \to \infty$.

(ii) *For* $n \geq 2$, *given an upper bound* $H_n \leq p^{1-\varepsilon_n}$ *on the Heilbronn sum, we have*

$$\ell_{p^{n-1}} \leq n(\log p)^{1+\frac{1-\varepsilon_n}{n-1}+o(1)}$$

as $p^n \to \infty$.

We note that the upper bound in (ii) for $n = 2$, using $H_2 \ll p^{\frac{5}{6}+o(1)}$, is slightly weaker than the bound in part (i). The estimate in (i) is the result of [18] mentioned before. For the convenience of the reader, we include a proof here. The estimate in (ii) for $n = 3$, using $H_3 \leq p^{1-\frac{29}{702}+o(1)}$, was obtained by Shteinikov [21, Thm. 16]. For $n \geq 4$, using the estimate for H_n in (1.4), from (ii) we obtain

$$\ell_{p^{n-1}} \leq n(\log p)^{1+\frac{1}{n-1}-\frac{3.269}{n-1}(\frac{34}{151})^n+o(1)}. \tag{6.1}$$

Proof. (i) The proof follows identically [2] (and its subsequent improvements), and so we sketch only the outline here. We start with the upper bound of [3, Lemma 12], which in the notation of Section 4 can be stated for any interval $\mathcal{I}$ of points in $\mathbb{Z}_{p^n}$:

$$|G_n \cap \mathcal{I}| \ll_\varepsilon \frac{(p-1)}{q}|\mathcal{I}| + \frac{|\mathcal{I}|}{q}\sum_{i=1}^{L} N_i\phi_i \tag{6.2}$$

with $h = \min\{q^{1+\varepsilon}/|\mathcal{I}|, q/2\}$. Using the upper bound in (5.2), we have, for $n = 2$,

$$|G_2 \cap \mathcal{I}| \ll_\varepsilon \frac{|\mathcal{I}|}{p^2}(p + h^{\frac{3}{4}}p^{\frac{3793}{4368}+o(1)} + hp^{\frac{257}{312}+o(1)}).$$

Taking $|\mathcal{I}| = \lfloor p^{2-\frac{575}{3276}+3\varepsilon}\rfloor$, we have $h \ll p^{\frac{575}{3276}-\varepsilon}$ and

$$|G_2 \cap \mathcal{I}| \ll_\varepsilon \frac{|\mathcal{I}|}{p}.$$

Next, let $\mathcal{I} = [1, M]$ with $M = \lfloor p^{2-\frac{575}{3276}+3\varepsilon}\rfloor$. Since $u^{p-1} \equiv 1 \pmod{p^2}$ for all $u \leq \ell_p$, the same is true for all integers in $\mathcal{I}$ comprised of prime factors $\leq \ell_p$.

By [9, Thm. 2.1], the number of such integers is at least $M^{1-\log\log M/\log \ell_p}$, and thus

$$M^{1-\log\log M/\log \ell_p} \ll M/p,$$

from which the theorem follows.

(ii) For $n \geq 3$, we follow the method of Section 3, taking (with M even) $\mathcal{I} = [1, M]$, $\mathcal{J} = [-\frac{M}{2}+1, \frac{M}{2}]$, $\alpha = 1_I * 1_J$. Noting that $\alpha(x) \geq M/2$ on $\mathcal{I}$, we obtain the upper bound

$$|G_n \cap \mathcal{I}| \leq \frac{2}{M}\sum_{x\in G_n}\alpha(x) \leq \frac{2}{M}(p^{-n}|G_n|M^2 + H_n M) < 2\frac{|\mathcal{I}|}{p^{n-1}} + 2H_n.$$

Say $H_n \leq p^{1-\varepsilon_n}$. Then with $M = \lceil p^{n-\varepsilon_n}\rceil$ we have $|G_n \cap \mathcal{I}| \leq 4\frac{M}{p^{n-1}}$ and so, as before,

$$M^{1-\log\log M/\log \ell_{p^{n-1}}} \leq 4M/p^{n-1},$$

from which we derive

$$\ell_{p^{n-1}} \leq n(\log p)^{1+\frac{1-\varepsilon_n}{n-1}+o(1)}$$

as $p^n \to \infty$. □

7. Asymptotic Formula for $T_k(G_n)$

For $k \in \mathbb{N}$, let G_n^{2k} denote the Cartesian product of G_n with itself $2k$-times and

$$\begin{aligned} &T_k(G_n)\\ &\quad = \#\{(\mathbf{x},\mathbf{y}) \in G_n^{2k} : x_1 + \cdots + x_k = y_1 + \cdots + y_k\}\\ &\quad = \#\left\{(\mathbf{x},\mathbf{y}) \in \mathbb{Z}^{2k} : 1 \leq x_i, y_i \leq p-1, \sum_{i=1}^{k} x_i^{p^{n-1}} \equiv \sum_{i=1}^{k} y_i^{p^{n-1}} \pmod{p^n}\right\}. \end{aligned}$$

In particular, $T_1(G_n) = |G_n|$, and $T_2(G_n)$ denotes the additive energy of the group G_n. As noted by Malykhin [14], we have the elementary estimate,

$$T_k(G_n) \leq T_k(G_{n-1}) \tag{7.1}$$

for any k, n with $n \geq 2$. The estimate follows from the observation that if $1 \leq x_i$, $y_i < p$ are integers such that

$$x_1^{p^{n-1}} + \cdots + x_k^{p^{n-1}} \equiv y_1^{p^{n-1}} + \cdots + y_k^{p^{n-1}} \pmod{p^n},$$

then, since $x_i^{p^{n-1}} \equiv x_i^{p^{n-2}} \pmod{p^{n-1}}$, we also have

$$x_1^{p^{n-2}} + \cdots + x_k^{p^{n-2}} \equiv y_1^{p^{n-2}} + \cdots + y_k^{p^{n-2}} \pmod{p^{n-1}}.$$

As noted in (5.1), Shkredov, Solodkova, and Vyugin established that $T_2(G_2) \ll p^{\frac{32}{13}}\log^{\frac{14}{13}} p$. In the next section we obtain $T_3(G_2) \ll p^{\frac{161}{39}}\log^{\frac{55}{39}} p$ and prove asymptotic results for $T_k(G_n)$. The key lemma needed for proving these is as follows.

LEMMA 7.1. *For any positive integers n, k, l with $k \geq l$, we have*

$$T_k(G_n) = (p-1)^{2k} p^{-n} + O(H_n^{2k-2l} T_l(G_n)),$$

where the constant in the big-O is less than 1.

Proof. We have, for $k \geq l$,

$$\begin{aligned} T_k(G_n) &= p^{-n} \sum_{\lambda=0}^{p^n-1} \sum_{\mathbf{x}\in G_n^k} \sum_{\mathbf{y}\in G_n^k} e_{p^n}(\lambda(x_1+\cdots+x_k-y_1-\cdots-y_k)) \\ &= p^{-n}|G_n|^{2k} + p^{-n} \sum_{\lambda=1}^{p^n-1} |S_n(\lambda)|^{2k} \\ &= p^{-n}|G_n|^{2k} + O\left(p^{-n} H_n^{2k-2l} \sum_{\lambda=1}^{p^n-1} |S_n(\lambda)|^{2l}\right) \\ &= (p-1)^{2k} p^{-n} + O(H_n^{2k-2l} T_l(G_n)). \end{aligned}$$

□

For $n = 2$, using $H_2 \ll p^{\frac{5}{6}} \log^{\frac{1}{6}} p$ and $T_2(G_2) \ll p^{\frac{32}{13}} \log^{\frac{14}{13}} p$ (though in fact much weaker bounds will do), from the lemma we obtain

$$T_k(G_2) = p^{2k-2} + O(p^{2k-3}) + O(p^{\frac{5}{3}k - \frac{34}{39} + o(1)})$$

for $k \geq 2$, and thus the asymptotic formula $T_k(G_2) \sim p^{2k-2}$ holds for $k \geq 4$. The asymptotic result for $n \geq 3$ is given in the next section.

In order to state our next lemma, we define

$$H_n' := \max_{p \nmid y} |S_n(y)|.$$

Plainly, for $n \geq 2$,

$$H_n = \max\{H_n', H_{n-1}\}.$$

The key lemma needed for estimating the higher-order Heilbronn sums is the well-known Hölder-type inequality relating H_n' to the $T_k(G_n)$ (see, e.g., [10]). A proof is provided in the Appendix for the convenience of the reader.

LEMMA 7.2. *For any positive integers n, k, l, we have*

$$H_n' \leq (p^n T_k(G_n) T_l(G_n))^{\frac{1}{2kl}} (p-1)^{1-\frac{1}{k}-\frac{1}{l}}.$$

8. Estimation of H_n and $T_k(G_n)$

From Lemma 7.1, Lemma 7.2, and (7.1) we obtain an iterative process for estimating successive H_n, $T_k(G_n)$, starting from estimates for H_2 and $T_2(G_2)$. We suppose that

$$H_2 \ll p^{\gamma}, \qquad T_2(G_2) \ll p^{\lambda} \tag{8.1}$$

and define

$$\beta := \max\{4, 2\gamma + \lambda\}. \tag{8.2}$$

From Lemma 7.1 we thus have $T_k(G_2) \sim p^{2k-2}$ for $k \geq 4$ and

$$T_3(G_2) = p^4 + O(H_2^2 T_2(G_2)) \ll p^{\beta}. \tag{8.3}$$

The exponents $\gamma = \frac{5}{6} + o(1)$, $\lambda = \frac{32}{13} + o(1)$ mentioned before give $\beta = \frac{161}{39} + o(1) = 4.1282\ldots$.

THEOREM 8.1. *Let* $\{\ell_n\}$ *and* $\{k_n\}$ *be the sequences of positive integers defined by*

$$\ell_2 := 4, \qquad \ell_3 := \left\lceil \frac{3\beta}{9-2\beta} \right\rceil, \qquad \ell_{n+1} := \left\lceil \left(\frac{8-\beta}{5-\beta}\right)\ell_n \right\rceil \quad \text{for } n \geq 3$$

and

$$k_2 := 3, \qquad k_3 := \left\lfloor \frac{3\beta}{9-2\beta} \right\rfloor, \qquad k_{n+1} := \left\lfloor \left(\frac{8-\beta}{5-\beta}\right)\ell_n \right\rfloor \quad \text{for } n \geq 3.$$

For $n \geq 2$, *we have* $T_k(G_n) \ll p^{2k-n}$ *for* $k \geq l_n$ *with* $T_k(G_n) \sim p^{2k-n}$ *for* $k > k_n$.

For $n \geq 3$, *we have*

$$H_n \ll p^{1-\varepsilon_n}, \qquad \varepsilon_n := \begin{cases} (9-2\beta)/18 & \text{for } n = 3, \\ (5-\beta)/6l_{n-1} & \text{for } n \geq 4. \end{cases}$$

Proof. From Lemma 7.2, (7.1), and (8.3) we have

$$H_3' \leq (p^3 T_3(G_3)^2)^{\frac{1}{18}} p^{\frac{1}{3}} = p^{\frac{1}{2}} T_3(G_3)^{\frac{1}{9}} \leq p^{\frac{1}{2}} T_3(G_2)^{\frac{1}{9}} \ll p^{\frac{1}{2}+\frac{\beta}{9}} = p^{1-\varepsilon_3}.$$

Since $\frac{1}{2} + \frac{\beta}{9} \geq \frac{1}{2} + \frac{4}{9} > \gamma$, we also have

$$H_3 = \max\{H_3', H_2\} \ll p^{1-\varepsilon_3}.$$

Hence, by Lemma 7.1, for $k \geq 3$, we get

$$\begin{aligned} T_k(G_3) &= (p-1)^{2k} p^{-3} + O(H_3^{2k-6} T_3(G_2)) \\ &= p^{2k-3} + O(p^{2k-4}) + O(p^{(\frac{1}{2}+\frac{\beta}{9})(2k-6)+\beta}). \end{aligned}$$

For $k > \frac{3\beta}{9-2\beta}$, the exponent $2k-3$ dominates, and we get $T_k(G_3) \sim p^{2k-3}$ with

$$T_k(G_3) \ll p^{2k-3}, \quad k \geq \ell_3, \quad \text{and} \quad T_k(G_3) \ll p^{(\frac{1}{2}+\frac{\beta}{9})(2k-6)+\beta}, \quad 3 \leq k < \ell_3,$$

establishing the case $n = 3$ of Theorem 8.1.

For $n > 3$, we proceed by induction. Suppose that, for a given n, we have already established that

$$H_n \ll p^{1-\varepsilon_n}, \tag{8.4}$$

$$T_k(G_n) \ll p^{2k-n} \quad \text{for } k \geq \ell_n. \tag{8.5}$$

Hence, by Lemma 7.2, (7.1), (8.3), and (8.5),

$$\begin{aligned} H_{n+1}' &\leq (p^{n+1} T_3(G_{n+1}) T_{l_n}(G_{n+1}))^{\frac{1}{6l_n}} p^{\frac{2}{3}-\frac{1}{l_n}} \\ &\leq (p^{n+1} T_3(G_2) T_{l_n}(G_n))^{\frac{1}{6l_n}} p^{\frac{2}{3}-\frac{1}{l_n}} \\ &\ll p^{\frac{n+1}{6l_n}} (p^{\beta})^{\frac{1}{6l_n}} p^{(2l_n-n)\frac{1}{6l_n}} p^{\frac{2}{3}-\frac{1}{l_n}} = p^{1-\frac{1}{l_n}(\frac{5-\beta}{6})} = p^{1-\varepsilon_{n+1}}, \end{aligned}$$

and thus, since $\varepsilon_{n+1} < \varepsilon_n$,

$$H_{n+1} = \max\{H'_{n+1}, H_n\} \ll p^{1-\varepsilon_{n+1}}.$$

Therefore, by Lemma 7.1 and (7.1), for $k \geq \ell_n$, we have

$$\begin{aligned} T_k(G_{n+1}) &= (p-1)^{2k} p^{-(n+1)} + O(H_{n+1}^{2k-2\ell_n} T_{\ell_n}(G_n)) \\ &= p^{2k-(n+1)}(1 + O(p^{-1}) + O(p^{1-\varepsilon_{n+1}(2k-2\ell_n)})). \end{aligned}$$

Consequently, for $k > \ell_n + \frac{1}{2\varepsilon_{n+1}} = (\frac{8-\beta}{5-\beta})l_n$, we have $T_k(G_{n+1}) \sim p^{2k-(n+1)}$ with

$$T_k(G_{n+1}) \ll p^{2k-(n+1)} \quad \text{for } k \geq l_{n+1}$$

and

$$T_k(G_{n+1}) \ll p^{2k-n-\frac{(5-\beta)}{6l_n}(2k-2l_n)} \quad \text{for } l_n \leq k < l_{n+1},$$

and we recover the claim of the theorem for $(n+1)$. □

In the following corollary we make the growth with n explicit.

COROLLARY 8.1. *For $n \geq 4$, we have*

$$H_n \ll_n p^{1-\frac{(5-\beta)^{n-3}}{6(l_3+(5-\beta)/3)(8-\beta)^{n-4}}}.$$

Proof. This follows at once from the bound

$$\begin{aligned} \ell_n &= \left\lceil \left(\frac{8-\beta}{5-\beta}\right)\ell_{n-1} \right\rceil \leq \left(\frac{8-\beta}{5-\beta}\right)\ell_{n-1} + 1 \\ &\leq \left(\frac{8-\beta}{5-\beta}\right)^{n-3} \ell_3 + \left(\frac{8-\beta}{5-\beta}\right)^{n-4} + \cdots + 1 \\ &= \ell_3 \left(\frac{8-\beta}{5-\beta}\right)^{n-3} + \left(\frac{5-\beta}{3}\right)\left(\left(\frac{8-\beta}{5-\beta}\right)^{n-3} - 1\right) \\ &< \left(\ell_3 + \frac{5-\beta}{3}\right)\left(\frac{8-\beta}{5-\beta}\right)^{n-3}. \end{aligned}$$

□

Thus, when $\beta = 161/39 + o(1)$, the optimal value currently available, we have $k_2 = 3$, $k_3 = 16$, $k_4 = 75$, $k_5 = 337, \ldots$, and $H_3 \ll p^{0.95868\ldots}$, $H_4 \ll p^{0.99145\ldots}$, $H_5 \ll p^{0.99808\ldots}, \ldots$, with $k_n \leq l_n \leq 0.1974(\frac{151}{34})^n$, and $H_n \ll p^{1-3.269(\frac{34}{151})^n}$.

Appendix: Proof of Lemma 7.2

We shall use the following version of Hölder's inequality.

LEMMA A.1. *For any nonnegative real numbers a_i, b_i, $1 \leq i \leq n$, and any positive real number ℓ, we have*

$$\sum_{i=1}^{n} a_i b_i \leq \left(\sum_{i=1}^{n} a_i\right)^{1-\frac{1}{\ell}} \left(\sum_{i=1}^{n} a_i^2\right)^{\frac{1}{2\ell}} \left(\sum_{i=1}^{n} b_i^{2\ell}\right)^{\frac{1}{2\ell}}.$$

First, we note that for any integer λ and positive integer k, we have

$$\begin{aligned}(p-1)\Big(\sum_{x\in G_n} e_{p^n}(\lambda x)\Big)^k &= \sum_{y\in G_n}\Big(\sum_{x\in G_n} e_{p^n}(\lambda yx)\Big)^k \\ &= \sum_{x_1\in G_n}\cdots\sum_{x_k\in G_n}\sum_{y\in G_n} e_{p^n}(\lambda y(x_1+\cdots+x_k)) \\ &= \sum_{b=0}^{p^n-1} n(b)\sum_{y\in G_n} e_{p^n}(\lambda yb),\end{aligned}$$

where

$$n(b) = \#\{(x_1,\dots,x_k) : x_i \in G_n, 1\le i\le k, x_1+\cdots+x_k = b\}.$$

By Lemma A.1 and the elementary identities

$$\sum_{b=0}^{p^n-1} n(b) = (p-1)^k \quad \text{and} \quad \sum_{b=0}^{p^n-1} n(b)^2 = T_k(G_n),$$

we obtain, for any positive integer l and integer λ with $p\nmid\lambda$,

$$\begin{aligned}&(p-1)\Big|\sum_{x\in G_n} e_{p^n}(\lambda x)\Big|^k \\ &\le \Big(\sum_{b=0}^{p^n-1} n(b)\Big)^{1-\frac{1}{l}}\Big(\sum_{b=0}^{p^n-1} n(b)^2\Big)^{\frac{1}{2l}}\Big(\sum_{b=0}^{p^n-1}\Big|\sum_{y\in G_n} e_{p^n}(\lambda yb)\Big|^{2l}\Big)^{\frac{1}{2l}} \\ &= (p-1)^{k(1-\frac{1}{l})} T_k(G_n)^{\frac{1}{2l}}(T_l(G_n)p^n)^{\frac{1}{2l}}.\end{aligned}$$

Dividing by $(p-1)$ and taking the kth root yield the lemma.

ACKNOWLEDGMENTS. The authors wish to thank Igor Shparlinski for his valuable discussions on this paper, in particular, for leading us to the improvement in Theorem 1.1 for $n=2$ and to the improvements in the estimates of the Fermat quotients. We also wish to thank the referee for his valuable comments and directing our attention to the recent work of Shteinikov [21], which has strong parallels with this work.

References

[1] J. Bourgain and M.-C. Chang, *Exponential sum estimates over subgroups and almost subgroups of Z^*Q, where Q is composite with few prime factors,* Geom. Funct. Anal. 16 (2006), no. 2, 327–366.

[2] J. Bourgain, K. Ford, S. V. Konyagin, and I. E. Shparlinski, *On the divisibility of Fermat quotients,* Michigan Math. J. 59 (2010), no. 2, 313–328.

[3] J. Bourgain, S. V. Konyagin, and I. E. Shparlinski, *Product sets of rationals, multiplicative translates of subgroups in residue rings, and fixed points of the discrete logarithm,* Int. Math. Res. Not. IMRN (2008), 1–29, Art. ID rnn 090.

[4] D. W. Boyd, *Speculations concerning the range of Mahler's measure,* Canad. Math. Bull. 24 (1981), 453–469.
[5] D. De Silva and C. Pinner, *The Lind–Lehmer constant for $\mathbb{Z}_p^n$,* Proc. Amer. Math. Soc. 142 (2014), no. 6, 1935–1941.
[6] A. Granville, *Some conjectures related to Fermat's last theorem,* Number theory, Banff, 1988, pp. 177–192, de Gruyter, New York, 1990.
[7] D. R. Heath-Brown, *An estimate for Heilbronn's exponential sum, analytic number theory,* Proceedings of a conference in honor of Heini Halberstam, pp. 451–463, Birkhäuser, Boston, 1996.
[8] D. R. Heath-Brown and S. V. Konyagin, *New bounds for Gauss sums derived from k*th *powers, and for Heilbronn's exponential sum,* Q. J. Math. 51 (2000), no. 2, 221–235.
[9] S. Konyagin and C. Pomerance, *On primes recognizable in deterministic polynomial time, the mathematics of Paul Erdös, I, 176–198,* Algorithms Combin., 13, Springer, Berlin, 1997.
[10] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications,* Cambridge Tracts in Math., 136, Cambridge University Press, Cambridge, 1999.
[11] D. H. Lehmer, *Factorization of certain cyclotomic functions,* Math. Ann. 34 (1933), 461–479.
[12] H. W. Lenstra, *Miller's primality test,* Inform. Process. Lett. 8 (1979), no. 2, 86–88.
[13] D. Lind, *Lehmer's problem for compact Abelian groups,* Proc. Amer. Math. Soc. 133 (2005), 1411–1416.
[14] Y. V. Malykhin, *Estimates of trigonometric sums modulo p^r,* Mat. Zametki 80 (2006), no. 5, 748–752, translated from, 80, 5, 2006, 793–796.
[15] H. L. Montgomery and R. C. Vaughan, *Exponential sums with multiplicative coefficients,* Invent. Math. 43 (1977), no. 1, 69–82.
[16] I. D. Shkredov, *On Heilbronn's exponential sum,* Q. J. Math. 64 (2012), no. 4, 1221–1230.
[17] ———, *On exponential sums over multiplicative subgroups of medium size,* Finite Fields Appl. 30 (2014), 72–87.
[18] I. D. Shkredov, E. V. Solodkova, and I. V. Vyugin, *Intersections of multiplicative subgroups and Heilbronn's exponential sum,* 6, pp. 1–22, 2015, May, arXiv:1302.3839v3 [math.NT].
[19] I. E. Shparlinski, *On the value set of Fermat quotients,* Proc. Amer. Math. Soc. 140 (2012), no. 4, 1199–1206.
[20] Y. N. Shteinikov, *Divisibility of Fermat quotients,* Translation of Mat. Zametki 92 (2012), no. 1, 116–122, 92, 2012, 1, 108–114.
[21] ———, *Estimates of trigonometric sums over subgroups and some of their applications,* Translation of Mat. Zametki 98 (2015), no. 4, 606–625, 98, 2015, 4, 667–684.

T. Cochrane
Department of Mathematics
Kansas State University
Manhattan, KS 66506
USA

cochrane@math.ksu.edu

D. De Silva
Department of Mathematics
Bowling Green State University,
Firelands
Huron, OH 44839
USA

dilumd@bgsu.edu

C. Pinner
Department of Mathematics
Kansas State University
Manhattan, KS 66506
USA

pinner@math.ksu.edu